AMENDMENTS TO THE CLAIMS

This Listing of Claims will replace all prior versions and listings of claims in this application.

Listing of Claims:

1. (Currently Amended) A method performed in a communication system including a plurality of nodes communicating in a shared network segment and at least one multicast channel in said shared network segment, the method comprising:

~~sending multicast messages from nodes on at least one multicast channel to other nodes;~~

providing a ~~further~~ specific multicast channel for sending jump-start messages by the nodes to said other nodes when a node has not received any regular start-up messages from other nodes on one or more multicast channels used for regular start-up messages;

sending a jump-start message on said specific multicast channel from a start ~~by using a start~~ node that has not received any regular start-up messages, wherein the jump-start message is secured by the start node and the start node starts an operation or an application;

receiving the jump-start message at a receiving node ~~the start message~~; and

validating an authenticity of the jump-start message upon receipt of the start message at the receiving node.

2. (Currently Amended) The method according to claim 1, wherein sending the jump-start message comprises monitoring by the start node for a predefined time to determine whether messages are sent on the specific multicast channel before sending the jump-start message from the start node.

3. (Currently Amended) The method according to claim 1, wherein sending the jump-start message comprises signing or encrypting by the start node the jump-start message using a key before sending the jump-start message.

4. (Currently Amended) The method according to claim 3, wherein sending the jump-start message comprises using the key comprising a private key of the start node.

5. (Original) The method according to claim 1, further comprising:

providing two further multicast channels for exchanging other messages different from multicast start messages.

6. (Currently Amended) The method according to claim 1, wherein sending the jump-start message comprises using the start node to start the application comprising an Open Shortest Path First protocol.

7. (Currently Amended) The method according to claim 1, further comprising:

sending the multicast messages from the nodes comprising routers including a Designated Router and other routers;

deciding that the Designated Router comprises an only available node in a shared segment if the Designated Router does not receive a response or the jump-start message from the other nodes when only the Designated Router comprises an active node in a shared network segment; and

generating a session key for at least one of authenticating or encrypting a further message by the Designated Router on another multicast channel when only the Designated Router comprises an active node in the shared network segment.

8. (Previously Presented) The method according to claim 7, wherein generating comprises using at least one of the public/private key pairs of the Designated Router for generating the session key for at least one of authenticating or encrypting the further message.

9. (Previously Presented) The method according to claim 7, wherein generating comprises generating the session key as a function of a Random Number, a private key, a public key, and a TimeStamp.

10. (Previously Presented) The method according to claim 7, wherein generating comprises using the session key as credential and applying the session key on a generated hello packet of an Open Shortest Path First protocol either for authentication or encryption.

11. (Currently Amended) The method according to claim 1, further comprising:

validating by the receiving node, when the receiving node receives the jump-start message from another node on the specific multicast channel, the jump-start message signed by a sending node; and

engaging in an Internet Key Exchange between the receiving node and the sending node to generate security associations.

12. (Previously Presented) The method according to claim 11, wherein engaging comprises using one of the security associations for unicast communication between the nodes, and using another one of the security associations for multicast communication for transmitting messages.

13. (Previously Presented) The method according to claim 1, further comprising:

sending the multicast messages from the nodes comprising routers including a Designated Router, a Backup Designated Router and other routers;

engaging the Designated Router and the Backup Designated Router in an Internet Key Exchange with a new node to generate a unicast security association between the new node and the Designated Router and between the new node and the Backup Designated Router when the start message is sent from the new node and both the Designated Router and the Backup Designated Router are active;

generating using the Designated Router a new session key for multicast communications; and

informing, using the Designated Router, the Backup Designated Router about the new session key using the unicast security association for communications between the Designated Router and the Backup Designated Router.

14. (Original) The method according to claim 1, further comprising:

generating a new session key for new nodes which connect and join an Open Shortest Path First network.

15. (Original) The method according to claim 1, further comprising:

providing a group communication mechanism, when a new node joins a group, an existing node leaves a group, group keys are changed, session keys are changed or new keys are distributed.

16. (Original) The method according to claim 1, further comprising:

generating using a Designated Router a new group key for all nodes when new Open Shortest Path First nodes join a network;

first distributing the new group key to a Backup Designated Router using the Designated Router;

next using the Designated Router and the Backup Designated Router to distribute the new key to all other nodes using respective unicast security association messages.

17. - 32. (Canceled)

33. (Currently Amended) A node for use in a system including at least one multicast channel on which the node can send multicast messages to other nodes, wherein the node is configured to:

send a start message on a specific multicast channel of a system when the node starts an operation or an application and when the node has not received regular start-up messages from other nodes on other multicast channels, wherein the start message is to be secured by the ~~a start~~ node.

34. (Original) The node according to claim 33 wherein said node, when starting the operation or the application, is configured to monitor for a predefined time to determine whether messages are sent on the specific multicast channel, before sending the start message from the node.

35. (Original) The node according to claim 33, wherein the node, before sending the start message, is configured to sign or encrypt the start message using a key.

36. (Previously Presented) The node according to claim 33, further comprising:

a router comprising a Designated Router;

the Designated Router being configured, after sending the start message, to decide that the Designated Router comprises an only available node in a shared segment, if the Designated Router does not receive a response or the start message from other nodes; and

the Designated Router being configured to generate a session key for at least one of authenticating and encrypting a further message by the Designated Router on another multicast channel.

37. (Original) The node according to claim 33, wherein the node comprises a router.

38. (Currently Amended) A method, comprising:

sending, by a node in a system including at least one multicast channel on which the node can send multicast messages to other nodes, a start message on a specific multicast channel of the system when the node starts an operation or an application and when the node has not received regular start-up messages from other nodes on other multicast channels, wherein the start message is secured by the ~~a start~~ node.

39. (Previously Presented) The method according to claim 38, further comprising monitoring by said node, when starting the operation or the application, for a predefined time to determine whether messages are sent on the specific multicast channel, before sending the start message from the node.

40. (Previously Presented) The method according to claim 38, further comprising signing or encrypting, by the node before sending the start message, the start message using a key.

41. (Previously Presented) The method according to claim 38, wherein the node comprises a router comprising a Designated Router, the method further comprising:

deciding, by the Designated Router after sending the start message, that the Designated Router comprises an only available node in a shared segment, if the Designated Router does not receive a response or the start message from other nodes; and

generating, by the Designated Router, a session key for at least one of authenticating and encrypting a further message by the Designated Router on another multicast channel.

42. (New) The method according to claim 1, wherein the regular start-up messages comprise at least one type of message selected from the group consisting of "Hello Protocol" messages and Link State Advertisement messages.

43. (New) The node according to claim 33, wherein the regular start-up messages comprise at least one type of message selected from the group consisting of "Hello Protocol" messages and Link State Advertisement messages.

44. (New) The method according to claim 38, wherein the regular start-up messages comprise at least one type of message selected from the group consisting of "Hello Protocol" messages and Link State Advertisement messages.

45. (New) The method according to claim 1, wherein said plurality of nodes comprises router nodes.

46. (New) The method according to claim 38, wherein the nodes comprise router nodes.